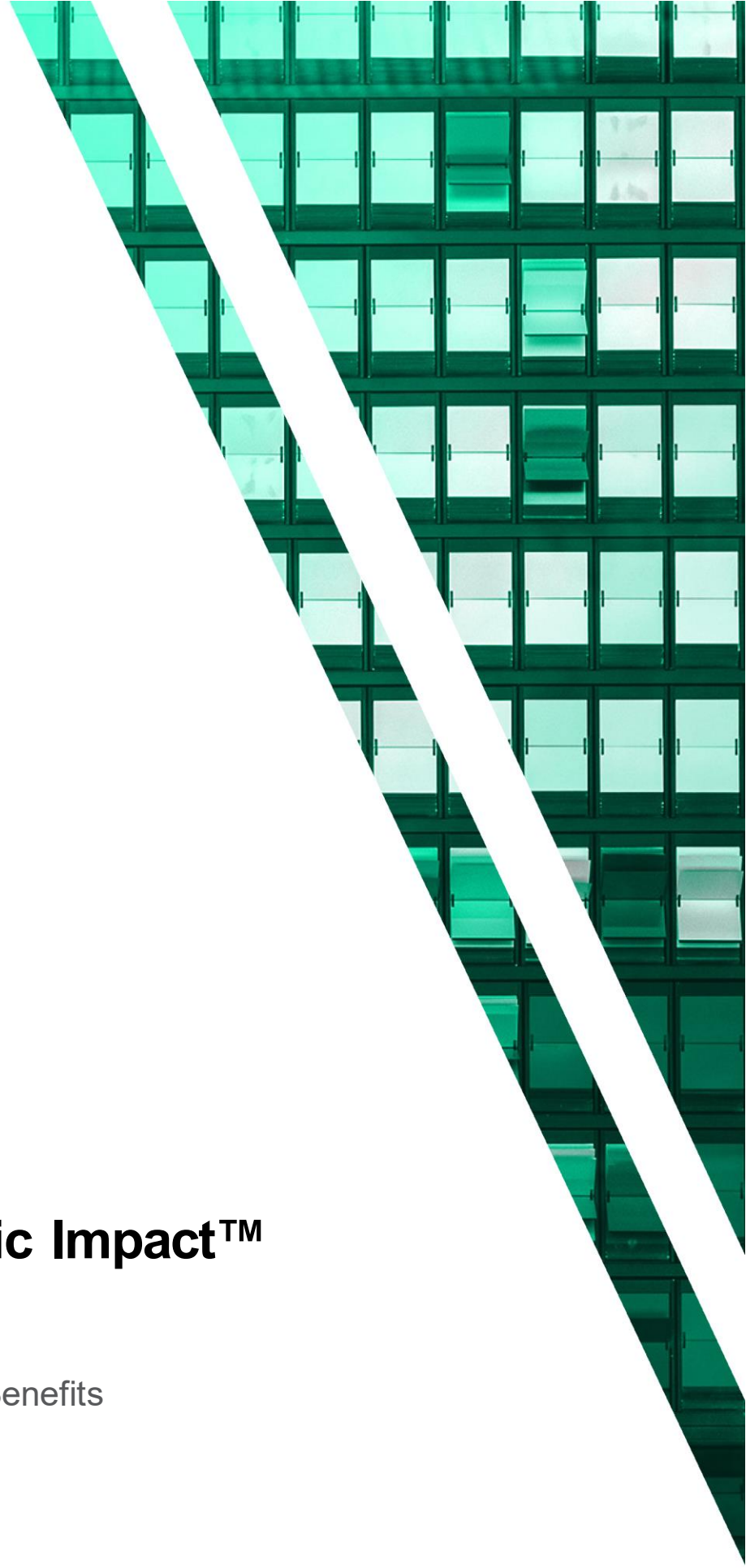
FORRESTER®



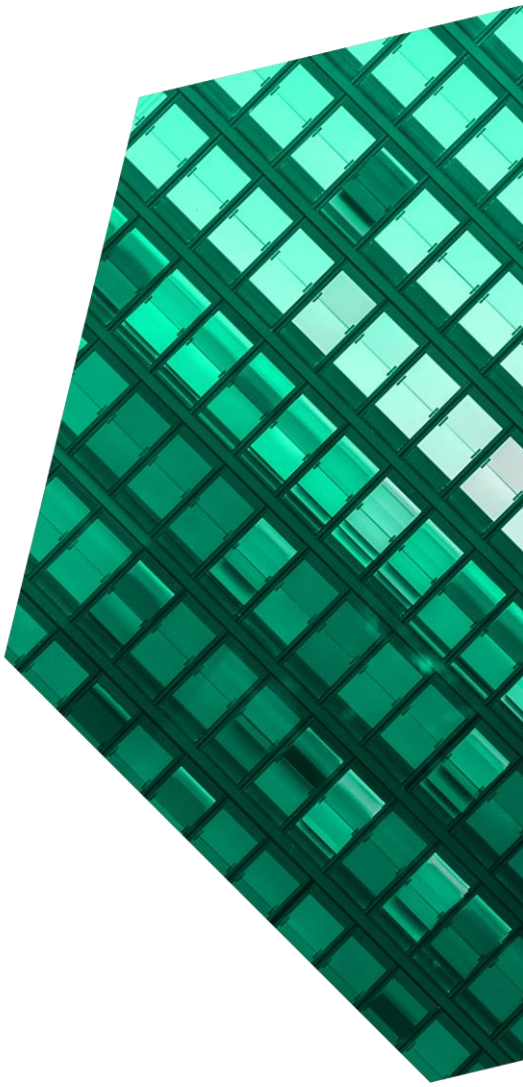
The Total Economic Impact™ Of Protegrity

Cost Savings And Business Benefits Enabled By Protegrity

JULY 2022

Table Of Contents

Consulting Team: Nick Ferrif
Tony Lam



ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

Executive Summary

Data is a business's greatest opportunity and, if not managed correctly, can be its greatest liability. Unlocking the potential value of organizational data without creating more risk can seem like a daunting task, but it is a necessary step for many businesses to remain competitive in their markets. Data protection platforms provide organizations with the tools and capabilities they need to unlock previously unusable data while guaranteeing the anonymity and security of that data.

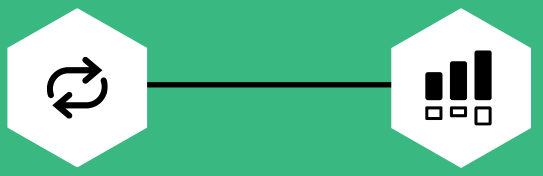
Protegrity is a data protection platform that allows businesses to secure, classify, and discover data while protecting it. With Protegrity, businesses can operationalize sensitive data through applications, advanced analytics, machine learning, and AI capabilities while keeping the data safe and compliant with industry regulations governing PII and the payment card industry. The ability to leverage new data sets or leverage data in new ways can help businesses accomplish a variety of goals including developing new products and revenue streams, enhancing sales and marketing techniques and effectiveness, and improving customer experience.

Protegrity commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Protegrity.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Protegrity on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed the decision-maker of an organization with experience using Protegrity. Forrester used this experience to project a three-year financial analysis.

Prior to using Protegrity, the interviewee noted how the organization did not have a centralized tool or service to advise application developers and architects on how to manage application and data security. Individual teams and lines of business (LOBs) were left to develop their own strategies, creating a patchwork of security tools and methodologies that was difficult to review or audit. Teams were often told "no" after requesting to leverage specific, sensitive data sets as part of their applications. Eventually, as the use cases for data grew more numerous, compelling, and potentially valuable to the business, the ability to leverage all organizational data and move data within the network became a requirement, forcing the organization to seek out a flexible solution that met the needs of the various LOBs.

KEY STATISTICS



Return on investment (ROI)
126%

Net present value (NPV)
$10.8 million

After the investment in Protegrity, the decision-maker's organization used Protegrity's technology to set up an as-a-service program for its LOBs. For this study, we will refer to the program as "Protegrity-as-a-Service" or "PaaS." PaaS is a REST API that allows everyone who onboards to the platform to use Protegrity as needed to secure data and ensure their application or service is both secure and compliant.

"The value of the investment in Protegrity is that it has enabled our LOBs to do things with data they could not have otherwise done — and do those things efficiently."

— Global senior vice president (SVP), financial services

Key results from the investment include efficiency gains for application builders and information security officers, reduced time-to-value for new applications and services, increased revenue from new income streams, reduced cost of compliance, and improved security.

KEY FINDINGS

Quantified benefits. Risk-adjusted present value (PV) quantified benefits include the following:

- **Efficiency gains for app builders reduce the time spent on security and compliance by 55%, representing $2.6 million in savings over three years.** With Protegrity, developers, architects, and security officers have a centralized tool with standardized policies, playbooks, and best practices to leverage, reducing the time, effort, and knowledge required to successfully and compliantly secure applications.

"In the past, it may have taken a team three days to redact data for a specific request. We can now do that in real time."

Global SVP, financial services

- **Cost savings from sunsetting legacy technology and infrastructure represent $1.8 million over three years.** With Protegrity as the backbone of the PaaS, the interviewee's organization sunsets legacy technology licenses while decommissioning legacy infrastructure.
- **Improved revenue from reduced time-to-value for applications and services and net-new income streams represents $13.7 million over three years.** The interviewee's organization streamlines the security review process for applications and services, accelerating the time-

to-value for all projects. Additionally, with Protegrity's ability to secure data at the source and make the data usable, LOBs can undertake new projects and develop new services that were not feasible before.

- **Reduced cost of compliance saves $1.3 million over three years.** With standardized practices and policies, compliance officers have a much easier time auditing and keeping the business compliant. Additionally, due to the way the PaaS program is designed and deployed, compliance officers are not required to keep the systems up to date with the latest local rules and regulations because sensitive data is never moved or directly accessed.

"We have opened many use cases that did not exist or were not possible before Protegrity."

Global SVP, financial services

Qualitative benefits. Benefits that are not quantified for this study include:

- **Improved data security.** With Protegrity's vaultless tokenization, organizations can abstract sensitive data so it is usable for analytics and other purposes but useless if a bad actor gets access or a copy of the data. With Protegrity, organizations have another line of defense against common cybersecurity threats like ransomware because data that has been protected by Protegrity is useless and harmless outside of the platform.

Costs. Risk-adjusted PV costs include:

- **Program development, deployment, and ongoing management costs of $2.1 million over three years.** Before deployment, the interviewee works with Protegrity to develop and test the PaaS program to ensure it meets a robust set of requirements from the business. Once developed, a small team of internal employees work with Protegrity to set up the program and develop all of the necessary collateral and training materials. Once up and running, five FTEs are in charge of managing the platform.
- **Infrastructure costs and training for PaaS of $697K over three years.** The interviewee's organization invests to build out the on-premises infrastructure necessary to support the PaaS program.
- **Protegrity licensing costs of $5.8 million.** The interviewee's organization requires $400,000 in professional services during initial setup and over the first year to ensure a smooth deployment and ongoing functionality. Additionally, the organization pays $2.5 million per year in licensing starting in Year 2 when the PaaS service is deployed globally.

Application builders spend **55% less time** on data security activities with Protegrity as the centralized solution

The interview and financial analysis found that the decision-maker's organization experiences benefits of $19.4 million over three years versus costs of $8.6 million, adding up to a net present value (NPV) of $10.8 million and an ROI of 126%.

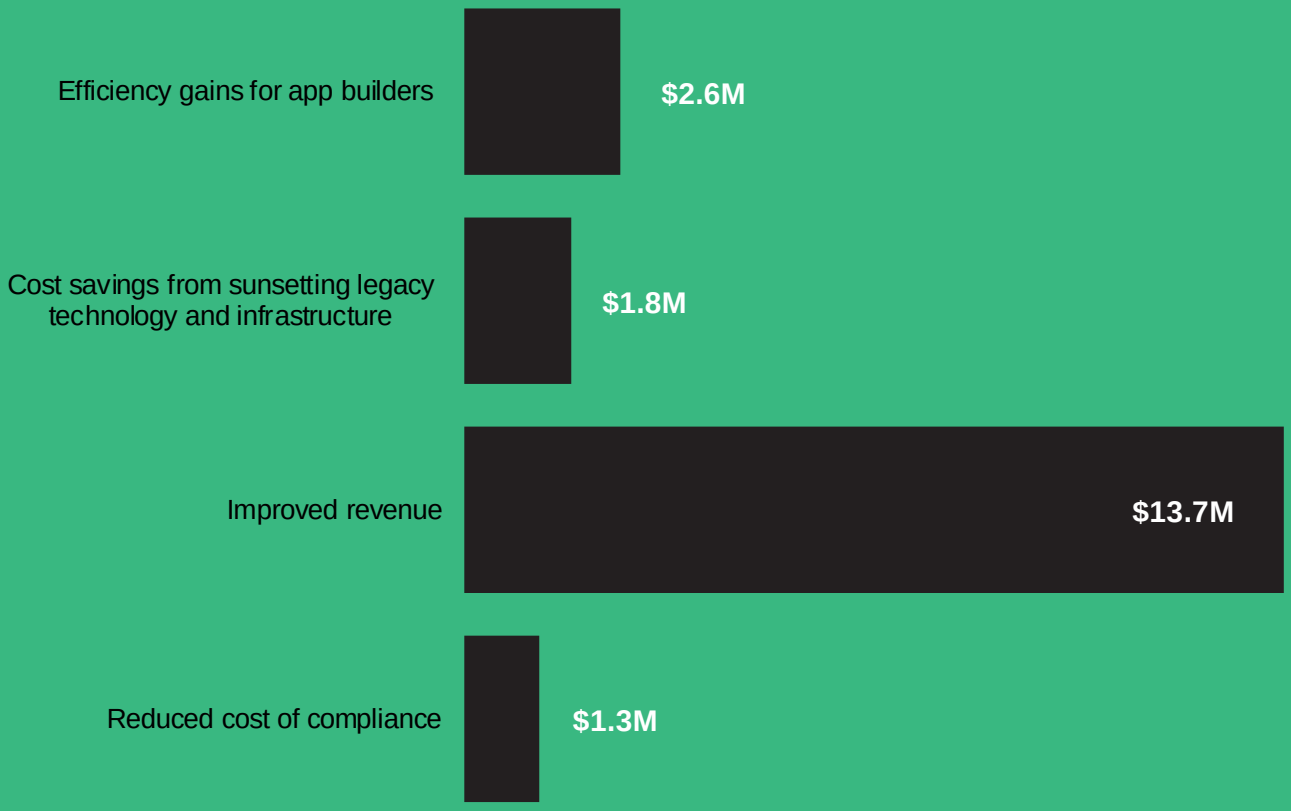
ROI
126%

BENEFITS PV
$19.4 million

NPV
$10.8 million

PAYBACK
8 months

Benefits (Three-Year)



TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Protegrity.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that Protegrity can have on an organization.

DUE DILIGENCE

Interviewed Protegrity stakeholders and Forrester analysts to gather data relative to Protegrity.

DECISION-MAKER INTERVIEW

Interviewed the decision-maker of an organization using Protegrity to obtain data with respect to costs, benefits, and risks.

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interview using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the decision-maker.

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Protegrity Customer Journey

Drivers leading to the Protegrity investment

INTERVIEWEE'S ORGANIZATION

Forrester interviewed the decision-maker of a financial services company whose organization has the following characteristics:

- More than $40 billion in annual revenue.
- US-based with global operations.
- More than 50,000 employees.
- On-premises infrastructure with no public cloud connection or use.

KEY CHALLENGES

Before investing in Protegrity for data security, the interviewee's organization did not have predefined best practices or a preferred tool to use to secure and/or obfuscate sensitive data. All LOBs and development teams had their own preferred method and tools and relied on the information security team to review their work and provide feedback if their data protection or security was lacking.

The interviewee's organization leverages on-premises infrastructure, with sensitive data stored regionally to ensure customer data security and compliance with all regional data security and privacy regulations. This architecture, and the ever-changing nature of regional regulations, made it extremely difficult for the organization to leverage its data in a meaningful way without jeopardizing data security, compliance, or both.

The interviewee noted how the organization struggled with common challenges, including:

- **Leveraging organizational data was difficult.** The organization needed the ability to leverage its data in meaningful ways without compromising security or violating any regional data security and protection regulations. Previous policies and infrastructure made it impossible to accommodate certain use cases or requests to use data, negatively impacting the client experience and causing the business to miss out on potential revenue streams.

  The interviewee explained: "We would receive requests from the different LOBs to leverage customer data in specific ways to achieve certain outcomes. Unfortunately, we had to decline many of these requests because, from a data security and information security level, we did not have the capabilities to enable that use case at that time."

> **"At a global level, it is very hard to support data movement. For example, if the data is part of a token vault that is in North America and someone in EMEA or APAC needs the data, how do we accommodate that? We started seeing similar business requirements and requests coming out of the different regions and decided that we needed to find a global solution for this issue."**
>
> *Global SVP, financial services*

- **Moving data became a business requirement, not a nice-to-have.** One of the key pillars of many global data privacy and security regulations is the concept of keeping customers' data in the same region, country, or sometimes even city

where they reside.[2] The interviewee's organization was set up to adhere to these regulations with regional on-premises infrastructure. However, challenges arose when it came time to leverage that data for analytics, marketing, product development, etc. There was a growing demand from the LOBs to move data around the organization to take advantage of advanced tools like business intelligence analytics, AI/ML, and automation.

- **Lack of consistent technology or a methodology for data security added complexity and created delays.** Teams were using ad hoc solutions for data security and protection with no centralized management or control, creating a patchwork landscape. Compliance officers and the information security team struggled to gain full visibility into data protection practices across the organization and to provide clear, concise feedback and recommendations to developers and app architects without a single centralized solution to rely on.

"Before Protegrity, there were a lot of different technologies and methodologies being used within these development teams and app teams. For data security, they would typically use a combination of redaction, anonymization, and masking, but it was all being done at different levels and with different tools depending on the organization."

Global SVP, financial services

- **Legacy technologies and methods became obsolete and expensive.** Token vaults, the primary legacy tokenization solution, were becoming too large and expensive for the organization to manage and no longer met the needs of the business. Additionally, as the use of organization data became more important and urgent for these initiatives, having older disparate tools made it challenging for data security and compliance officers to accommodate business requests and provide simple, workable solutions for data usage requests.

  The interviewee said: "The problem with vaulted tokenization is, as your data field grows, your vault grows. And so you end up with these massive unsupportable databases of sensitive data that might take 10 minutes to run a single query. We also want to avoid storing sensitive data whenever possible. With Protegrity, all of this comes off the table."

- **There was no ability to leverage advanced analytics and business insights tools.** Because organizational data is siloed regionally and difficult to move, the organization could only perform analytics on small slices of data, significantly limiting the usefulness and impact. This became untenable as the benefits and business advantages of performing big data analysis became clearer.

  The interviewee said: "We had a lot of third-party vendors coming to our LOBs to pitch analytics and marketing tools using AI and cutting-edge ML models to predict customer needs, improve marketing, and so on. There was a need coming from the business of wanting to leverage some of these tools that we looked to accommodate with this investment in Protegrity."

INVESTMENT OBJECTIVES

The interviewee was looking not simply to adopt a technology to solve the data protection and data movement challenges but also to establish a centralized platform for data security that could accommodate all LOBs and use cases with a small team of dedicated experts.

The interviewee's organization searched for a solution that could:

- **Meet the diverse needs and requirements laid out by the businesses and LOBs.** The interviewee explained: "We had a very robust set of requirements sourced from multiple LOBs from multiple regions and countries that served as our initial barometer for success. We wanted to come back to the business with an architecture or technology and solution that met the requirements. And those requirements ranged all the way from business requirements to app dev requirements and our own data protection and security requirements."
- **Be flexible enough to handle future unknown requirements, requests, and data privacy and protection regulations.** The interviewee recognized that while data protection laws will continue to change, the core principle of data residency is consistent. So the interviewee wanted to develop a solution that ensured that local data never left its area of origin and that never violated data residency requirements.

  The interviewee said: "The format preservation and data movement capability of vaultless tokenization certainly started to answer a lot of the questions and requirements that we had coming at us. Ultimately, we saw a path forward with Protegrity's technology, so we engaged it to help build out this service."

WHY PROTEGRITY?

After an RFP and business case process evaluating multiple vendors, the interviewee's organization chose Protegrity for the following reasons:

- **Vaultless tokenization and Protegrity's underlying technology and capabilities.** Vaultless tokenization's format preservation and data movement capabilities solved many complex needs coming from the LOBs and business leaders. Also, the ability to leverage other data protection or obfuscation methods for different use cases on the same platform provided the flexibility those same LOBs needed to solve any other niche needs or use cases.

  The interviewee said: "With Protegrity, we can offer our developers a centrally managed runtime API that gives them the tools and flexibility to build secure compliant applications and processes with minimal effort. And from a cybersecurity and data security standpoint, we can actually see and track what is happening."
- **Technological fit and customer service.** Protegrity worked closely with the interviewee to develop the technology to meet specific needs and to build out the PaaS practice. The interviewee said: "At the time we initially reached out, Protegrity didn't even offer the specific technology that we needed to build out the service. Protegrity brought in the head of development and some engineers to pitch the Data Security Gateway product, and something immediately clicked with me. So I worked with them to build out the specific requirements that we were looking for and developed our PaaS program."
- **Ability to meet data security and flexibility needs**. The interviewee said, "What it boils down to is the actual operation of tokenization only occurs in memory in the country and city network that you want."

"Through this service, I can guarantee that this data never leaves a particular entity and can satisfy any regulatory requirements. Using Protegrity, I can make those guarantees for our LOBs."

Global SVP, financial services

USE CASE DESCRIPTION

The interviewee's organization is a US-based global financial services organization with more than 50,000 employees globally. The organization has multiple LOBs including consumer and institutional banking services.

The interviewee recognized the potential value in Protegrity's vaultless tokenization and worked with Protegrity to develop the PaaS program for the business. The idea behind the PaaS program was to give application builders a standardized set of tools to reduce the complexity involved with data protection and to standardize processes across the organization.

Additionally, the interviewee wanted to set up an infrastructure that would comply with current data protection and privacy laws and, by securing data at its source, future data residency laws by ensuring that local data never left its local environment.

The organization deploys 100% on-premises infrastructure and does not leverage any public cloud services or capabilities. This 100% on-premises deployment can operate similarly to a private cloud in certain instances and is the reason the organization deploys Protegrity and the PaaS program on-premises with physical infrastructure.

After the initial development and testing period, one LOB onboards in Year 1 and fully leverages the capabilities of Protegrity and the PaaS program. During the first few months, the LOB updates any existing projects/use cases to leverage Protegrity technology and then develops net-new use cases leveraging data sources that were not previously accessible or usable.

Additional LOBs onboard in Years 2 and 3, and as the use of Protegrity and the PaaS program grows, the need to leverage legacy data security tools diminishes, allowing the organization to sunset those legacy solutions and remove obsolete infrastructure.

Each use case represents more than $10 million in revenue for the business, and use cases can vary from offering an entire new product or service to decommissioning an old product at the correct time by leveraging customer data that was not previously available.

It should be noted that while the interviewee's organization is 100% on-premises, Protegrity also supports cloud and hybrid infrastructure. The benefits described in this study are relevant for other organizations that leverage different infrastructure architectures.

Key assumptions

- **More than $40 billion in annual revenue**
- **More than $10 million per project/use case**
- **More than 50,000 total employees**

Analysis Of Benefits

Quantified benefit data

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Efficiency gains for app builders	$237,006	$1,185,030	$1,896,048	$3,318,084	$2,619,353
Btr	Cost savings from sunsetting legacy technology and infrastructure	$410,400	$627,000	$1,174,200	$2,211,600	$1,773,467
Ctr	Improved revenue	$2,435,577	$6,227,885	$8,434,615	$17,098,077	$13,698,224
Dtr	Reduced cost of compliance	$262,656	$525,312	$787,968	$1,575,936	$1,264,932
	Total benefits (risk-adjusted)	$3,345,639	$8,565,227	$12,292,831	$24,203,697	$19,355,976

EFFICIENCY GAINS FOR APP BUILDERS

Evidence and data. Developers, application architects, and data security teams saved time and effort with Protegrity as their data security tool. The ability to leverage playbooks, provide specific feedback and guidance for updates, as well as use a centralized platform for all of this work reduced the time that these teams spent on data security reviews, allowing them to focus their efforts on more valuable tasks.

- Prior to Protegrity and PaaS, the interviewee's organization relied on the data and information security teams to review new applications and services to ensure they met data security standards and provide feedback where the protections fell short. Application builders had access to multiple tools and techniques, including vaulted tokenization and encryption, and there were no centralized processes or commonly followed best practices. So reviews were complex, and feedback from the information and data security teams often lacked specific instructions for improvement.
- Once the PaaS program deployed, each onboarded LOB had a centralized data security solution that included playbooks and best practices, reducing the time and effort required to implement the data security measures and streamlining the process to review and approve new applications and services.
- The interviewee said: "Once the plumbing is set up and the LOB is onboarded, they have the capability to tokenize and detokenize anything they want essentially. They specify the source of data that they want something done to. They specify how to extract the data out of that source. They identify what level of protection that they want. They can define all of these things at runtime, and the PaaS program team never has to get involved."

Modeling and assumptions. For the financial model, Forrester assumes:

- There are 60 FTEs per LOB that leverage Protegrity and the PaaS program. One LOB onboards in Year 1, with five LOBs onboarded by Year 2 and eight LOBs onboarded by Year 3.
- Prior to Protegrity and PaaS, the application builders spend 5% of their time working on data security and protection.
- Protegrity acting as a centralized solution for data security and tokenization reduces the labor involved with data security and protection by 55%.
- The average fully loaded salary for application builders is $216,000 per year.
- Protegrity accounts for 70% of the benefits realized, with 30% of the benefits attributed to the individuals involved and the workstreams that were set up to accommodate the PaaS program.

Risks. The results of the financial model can vary due to:

- The number of application builders impacted by deploying Protegrity.
- The percentage of time spent building data security and compliance into new applications and services.
- The impact that Protegrity has on streamlining the building and review process.
- Average salaries.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV (discounted at 10%) of $2.6 million.

Efficiency Gains For App Builders

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Number of developers, application architects, and information security officers that leverage Protegrity/PaaS	Forrester assumption	60	300	480
A2	Time spent on building/updating application security and compliance before Protegrity	Forrester assumption	5%	5%	5%
A3	Efficiency gains for developers in app security and compliance	Interviews	55%	55%	55%
A4	Average salary of developer, app architect, or information security officer	$160,000*1.35	$216,000	$216,000	$216,000
A5	Productivity capture	Forrester assumption	70%	70%	70%
At	Efficiency gains for app builders	A1*A2*A3*A4*A5	$249,480	$1,247,400	$1,995,840
	Risk adjustment	↓5%			
Atr	Efficiency gains for app builders (risk-adjusted)		$237,006	$1,185,030	$1,896,048
	Three-year total: $3,318,084			**Three-year present value: $2,619,353**	

COST SAVINGS FROM SUNSETTING LEGACY TECHNOLOGY AND INFRASTRUCTURE

Evidence and data. As more LOBs onboarded to the PaaS solution, the need to use other technologies and solutions decreased. Once onboarded, an LOB no longer needed the legacy tools and solutions that it relied on in the past, allowing the organization to reduce licenses and remove or repurpose infrastructure.

- Prior to building the PaaS program with Protegrity, the interviewee's organization used on-premises token vaults to store tokenization data. As tokenization was used more widely, the number and size of the token vaults continued to grow, eventually becoming too big and expensive to properly manage. Additionally, the organization did not want to store sensitive data if avoidable, and the token vaults represented a significant source of risk if a breach or other cybersecurity incident occurred.
- Once onboarded to the PaaS program with Protegrity, LOBs no longer needed to leverage legacy solutions, giving up their licenses and decommissioning old token vaults once their data security migrated to Protegrity.

Modeling and assumptions. For the financial model, Forrester assumes:

- The organization has five active token vaults when it adopts Protegrity, with the intention of adding two more over the next three years.
- The organization decommissions 20% of the token vaults in Year 1, with 70% of the token vaults decommissioned by Year 3.
- In addition to decommissioning old token vaults, because LOBs now leverage Protegrity and the PaaS program, the organization no longer needs to build additional token vaults, saving on startup and infrastructure costs for new token vaults.
- Once onboarded, the organization sunsets $100 per user per month in security licenses related to legacy tools used for encryption, tokenization, anonymization, and masking.

Risks. The results of the financial model can vary due to:

- The specific legacy technologies used prior to deploying Protegrity.
- The speed at which an organization can deploy Protegrity across the business.
- The cost of legacy security licenses that the organization sunsets.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of $1.8 million.

"With our legacy solution, we may have been required to fully redact certain lines of data. With Protegrity, we can now use multicolumn vaultless tokenization to secure the specific points that we need while preserving the data and ensuring the process is reversable so we can actually leverage that data set for analytics or other use cases."

Global SVP, financial services

Cost Savings From Sunsetting Legacy Technology And Infrastructure					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Number of token vaults (on-premises) prior to Protegrity	Forrester assumption	5	5	5
B2	Annual operating cost per vault (labor, hardware, software, utilities)	Forrester assumption	$120,000	$120,000	$120,000
B3	Token vaults sunsetted with Protegrity/PaaS	Forrester assumption	20%	50%	70%
B4	Subtotal: savings from sunsetting token vaults	B1*B2*B3	$120,000	$300,000	$420,000
B5	Token vaults avoided due to Protegrity/PaaS deployment	Interviews	1		1
B6	Setup costs	Forrester assumption	$120,000	$120,000	$120,000
B7	Subtotal: savings from avoided token vaults	B5*(B6+B2)	$240,000	$0	$240,000
B8	Legacy security tools no longer used (per user per month)	Forrester assumption	$100	$100	$100
B9	Subtotal: legacy security license savings	B8*A1*12	$72,000	$360,000	$576,000
Bt	Cost savings from sunsetting legacy technology and infrastructure	B4+B7+B9	$432,000	$660,000	$1,236,000
	Risk adjustment	↓5%			
Btr	Cost savings from sunsetting legacy technology and infrastructure (risk-adjusted)		$410,400	$627,000	$1,174,200
	Three-year total: $2,211,600			**Three-year present value: $1,773,467**	

IMPROVED REVENUE

Evidence and data. With Protegrity, the organization used its data to drive innovation and find new income streams.

- The interviewee's organization adhered to very strict and diverse global data protection and privacy regulations. With the legacy solution, these regulations severely restricted how and where organizational data could be used, limiting innovation and preventing data and analytics teams from fully realizing their value to the organization. Requests to use certain data sets were often rejected because the technology did not exist to leverage the data in a secure and compliant way. And even when a data source could be used, it often took multiple days to anonymize data so it was usable for analytics and other purposes.
- With Protegrity and the PaaS program, the organization unlocked its data, allowing LOBs to leverage data that they did not previously have access to, opening up new use cases, enabling the use of AI and ML tools, and reducing the barriers to innovation for application builders.
- Examples of net-new use cases and revenue streams through Protegrity and the PaaS program include: 1) enabling the use of advanced marketing technology, business analytics, and other AI and ML technologies; 2) capturing and leveraging user and traffic data from global websites to draw insights and improve security; 3) giving customer service representatives

access to global customer records so they can serve any customer from anywhere; 4) establishing and successfully running customer rewards and loyalty programs; 5) developing new products, adjusting current offerings, and making faster go/no-go decisions; and 6) securely sharing data with outside partners and trusted third parties.

- In addition to the net-new use cases, the organization updates any currently running workstreams or products to leverage Protegrity rather than the legacy data protection solution.

Modeling and assumptions. For the financial model, Forrester assumes:

- One LOB onboards in Year 1, with five LOBs onboarded by Year 2 and eight LOBs onboarded by Year 3.
- Each LOB runs an average of three ongoing use cases/products annually. These are workstreams that repeat annually.
- Prior to Protegrity and the PaaS program, the organization spent an average of two weeks to develop and review data security practices of each new program/use case. With Protegrity, the review effort decreased by 75% because of a standardized platform.
- In Year 1, the organization takes on two net-new projects/use cases that were not possible before deploying Protegrity. In Year 2 and 3, the organization takes on three net-new projects/use cases that were previously not possible.
- Each project/use case is worth $10 million annually to the business.
- For net-new use cases enabled by Protegrity, 10% of the benefit of each use case is attributed to Protegrity for enabling the use of the data. The other 90% is attributed to the people, processes, and other technologies involved with building out the specific service, product, or capability.

"We have use cases where an LOB used the tokenization service to move data into the analytics world as pseudonymized data. When an event occurs within our analytics, that event can go back to the source as a pseudonymized event and detokenized so we can see the insights and take the appropriate action."

Global SVP, financial services

Risks. The results of the financial model can vary due to:

- The speed at which new LOBs onboard and the number projects each LOB runs concurrently.
- The extent to which corporate data use was restricted prior to deploying Protegrity.
- The value that each project represents to the overall business.
- The speed and maturity of the data security review process prior to investment.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of $13.7 million.

Improved Revenue					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Number of LOBs leveraging PaaS	Interviews	1	5	8
C2	Average number of use cases/projects within each LOB (annually)	Forrester assumption	3	3	3
C3	Annual value of each newly launched project/use case	Forrester assumption	$10,000,000	$10,000,000	$10,000,000
C4	Expected revenue per week	C3/52	$192,308	$192,308	$192,308
C5	Average time spent on data security and compliance reviews before Protegrity (weeks)	Forrester assumption	2	2	2
C6	Improvement with Protegrity	Forrester assumption	75%	75%	75%
C7	Subtotal: incremental revenue from improved time-to-value	C1*C2*C4*C5*C6	$865,385	$4,326,923	$6,923,077
C8	Number of new projects enabled by Protegrity (annually)	Interviews	2	3	3
C9	Attribution to Protegrity/PaaS	Forrester assumption	10%	10%	10%
C10	Subtotal: incremental revenue from net-new projects enabled by Protegrity	C8*C3*C9	$2,000,000	$3,000,000	$3,000,000
Ct	Improved revenue	C7+C10	$2,865,385	$7,326,923	$9,923,077
	Risk adjustment	↓15%			
Ctr	Improved revenue (risk-adjusted)		$2,435,577	$6,227,885	$8,434,615
Three-year total: $17,098,077			**Three-year present value: $13,698,224**		

REDUCED COST OF COMPLIANCE

Evidence and data. The PaaS program with Protegrity was designed to secure data at its source before being tokenized and leveraged around the organization. A key advantage to this architecture was that the data never left the local network so the organization could comply with local data residency regulations even though the program deployed globally.

- Prior to deploying Protegrity, the interviewee's organization used a variety of tools and methodologies for securing data, with the ultimate strategy and architecture typically determined by the application builder. This lack of standardization meant that each compliance review required net-new detailed analysis and recommendations.
- With Protegrity powering the PaaS program, the organization standardized data security practices, significantly reducing the amount of time and effort required to review each project/use case for compliance.

Modeling and assumptions. For the financial model, Forrester assumes:

- The organization employs 16 FTE compliance officers responsible for reviewing compliance to data security and privacy regulations.
- In Year 1, this team sees a 20% efficiency gain, growing to a 60% gain when more LOBs onboard to the platform.
- The average fully loaded annual salary for compliance officers is $108,000
- Protegrity is responsible for 80% of this benefit with the other 20% attributed to the people and processes put in place surrounding the compliance review process.

Risks. The results of the financial model can vary due to:

- The size of the compliance team and average annual salary.
- The impact that standardizing data protection practices will have on compliance reviews.
- The speed at which the organization adopts Protegrity.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of $1.3 million.

Reduced Cost Of Compliance

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Number of FTEs managing compliance, monitoring data movement, etc.	Forrester assumption	16	16	16
D2	Reduced effort to monitor and manage compliance	Forrester assumption	20%	40%	60%
D3	Average salary for compliance officer	$80,000*1.35	$108,000	$108,000	$108,000
D4	Attribution to Protegrity	Forrester assumption	80%	80%	80%
Dt	Reduced cost of compliance	D1*D2*D3*D4	$276,480	$552,960	$829,440
	Risk adjustment	↓5%			
Dtr	Reduced cost of compliance (risk-adjusted)		$262,656	$525,312	$787,968
	Three-year total: $1,575,936			**Three-year present value: $1,264,932**	

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Protegrity and later realize additional uses and business opportunities, including:

The ability to leverage virtually any data source regardless of location and content. Most businesses are just starting to scratch the surface in realizing the value of their organizational data. As new data sources become available and as new analytics techniques are developed, organizations that leverage Protegrity will have an easier time using data in a secure and compliant way while adhering to any global data protection and privacy laws.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

Analysis Of Costs

Quantified cost data

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	Program development, deployment, and ongoing management costs	$237,600	$772,200	$742,500	$742,500	$2,494,800	$2,111,088
Ftr	Infrastructure costs and training	$227,934	$102,354	$207,270	$272,832	$810,390	$697,263
Gtr	Protegrity licensing costs	$0	$1,732,500	$2,677,500	$2,625,000	$7,035,000	$5,760,011
	Total costs (risk-adjusted)	**$465,534**	**$2,607,054**	**$3,627,270**	**$3,640,332**	**$10,340,190**	**$8,568,362**

PROGRAM DEVELOPMENT, DEPLOYMENT, AND ONGOING MANAGEMENT COSTS

Evidence and data. The interviewee worked closely with Protegrity to develop and test the PaaS program to ensure it met a robust set of requirements from the business. Once rolled out, an internal team of five FTEs managed the program full-time.

- The interviewee, working with Protegrity, spent nine months developing the vision, building out the capabilities of the PaaS program, and ensuring it met a long list of solution requirements from leadership and LOBs.
- Once developed, the interviewee and his team built out the background materials necessary for launch including best practices playbooks for data security, onboarding materials and methodology, internal communications, and change management.
- During the first year, the interviewee spent two months tweaking and refining the PaaS program before passing the management over to his team of five internal FTEs.

Modeling and assumptions. For the financial model, Forrester assumes:

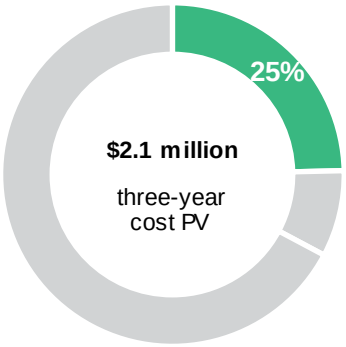
- One FTE is involved in the program codevelopment phase for nine months initially and another two months in Year 1.
- The annual fully burdened salary of this FTE is $162,000.
- A team of seven FTEs develops program materials initially.
- This team scales down to five once fully deployed in Years 1, 2, and 3 and is responsible for managing the platform and its users.
- The average loaded salary for the PaaS management team is $135,000 a year.

Risks. Risks that could impact the realization of this benefit include:

- The amount of time and effort dedicated to cocreation, development of internal materials, testing, and deployment.
- The amount of time employees take to familiarize themselves with the solution.

- The average fully burdened salaries for overall business and for IT.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year risk-adjusted total PV (discounted at 10%) of $2.1 million.



Program Development, Deployment, And Ongoing Management Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	FTEs for initial program codevelopment	Interviews	1	1		
E2	Time spent on initial codevelopment (months)	Interviews	9	2		
E3	Fully burdened salary	$120,000*1.35	$162,000	$162,000		
E4	Subtotal: program development and technology deployment	E1*(E2/12)*E3	$121,500	$27,000		
E5	FTEs helping with development of program materials, deployment, and ongoing management	Interviews	7	5	5	5
E6	Time spent dedicated to PaaS deployment, creating materials, etc.	Interviews	10%	100%	100%	100%
E7	Fully burdened salary of PaaS team	$100,000*1.35	$135,000	$135,000	135,000	135,000
E8	Subtotal: materials creation, testing, and deployment	E5*E6*E7	$94,500	$675,000	$675,000	$675,000
Et	Program development, deployment, and ongoing management costs	E4+E8	$216,000	$702,000	$675,000	$675,000
	Risk adjustment	↑10%				
Etr	Program development, deployment, and ongoing management costs (risk-adjusted)		$237,600	$772,200	$742,500	$742,500
	Three-year total: $2,494,800			**Three-year present value: $2,111,088**		

INFRASTRUCTURE COSTS AND TRAINING

Evidence and data. The interviewee's organization runs 100% on-premises and invested to build out the on-premises infrastructure necessary to support the PaaS program.

- The interviewee explained that both hardware and software costs were involved to get the PaaS program up and running.
- The interviewee noted that due to the ease of use of the Protegrity solution and support from Protegrity team members, training was minimal.

Modeling and assumptions. For the financial model, Forrester assumes:

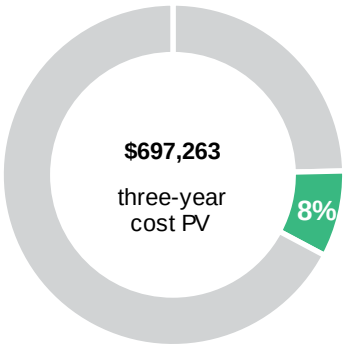
- Hardware costs to set up and support the PaaS program including purchasing servers and other associated hardware are $200,000 in the initial setup period.

- It costs $60,000 per year to maintain the hardware infrastructure including replacing hardware and expanding capacity when necessary.
- Software costs to set up and support the PaaS program start at $15,000 while developing the program and standing up the technology. The software costs increase annually as more users onboard and begin leveraging the platform.
- There is minimal training required for users to leverage Protegrity. The organization requires each application builder to undergo 2 hours of training during the onboarding process.
- Ten FTEs are trained initially, and then training occurs as users onboard.
- The average burdened salary of those FTEs is $104 an hour.

Risks. Risks that could impact the realization of this benefit include:

- The size and specific capabilities of the Protegrity deployment.
- The time required to train employees to use and understand Protegrity effectively.
- The cost of setting up and maintaining hardware and software.
- The nature of the deployment (on-premises, cloud, hybrid, etc.).

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $697K.



Infrastructure Costs And Training

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Hardware costs to set up and support PaaS	Forrester assumption	$200,000	$60,000	$60,000	$60,000
F2	Software costs to set up and support PaaS (security, IAM, support, etc.)	Forrester assumption	$15,000	$25,000	$75,000	$100,000
F3	Training hours required per onboarded FTE	Interviews	2	2	2	2
F4	FTEs trained	A1	10	60	300	480
F5	Average salary (hourly)	A4	$104	$104	$104	$104
F6	Subtotal: training costs	F3*F4*F5	$2,080	$12,480	$62,400	$99,840
Ft	Infrastructure costs and training	F1+F2+F6	$217,080	$97,480	$197,400	$259,840
	Risk adjustment	↑5%				
Ftr	Infrastructure costs and training (risk-adjusted)		$227,934	$102,354	$207,270	$272,832
	Three-year total: $810,390			**Three-year present value: $697,263**		

PROTEGRITY LICENSING COSTS

Evidence and data. Protegrity's license costs covered the interviewee's PaaS solution and were calculated based on the number of regions that the technology was operating in.

- The organization leveraged Protegrity's professional services to ensure a smooth initial deployment, with a smaller contract in subsequent years to help with expansion and to build out new capabilities.
- Costs were reported to be straightforward and predictable.

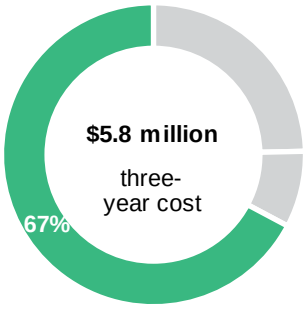
Modeling and assumptions. For the financial model, Forrester assumes:

- The initial setup fee for professional services in Year 1 is $400,000, with an additional $50,000 in Year 2 to ensure smooth scaling.
- The licensing fee in Year 1 is $1.25 million, increasing to $2.5 million annually once Protegrity and the PaaS program deploy globally.
- The organization processes 100 million requests per month. A request represents the need to tokenize/detokenize a specific value.

Risks. Risks that could impact the realization of this benefit include:

- The size and scope of the Protegrity deployment.
- The amount of professional services needed to stand up the solution.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $5.8 million.



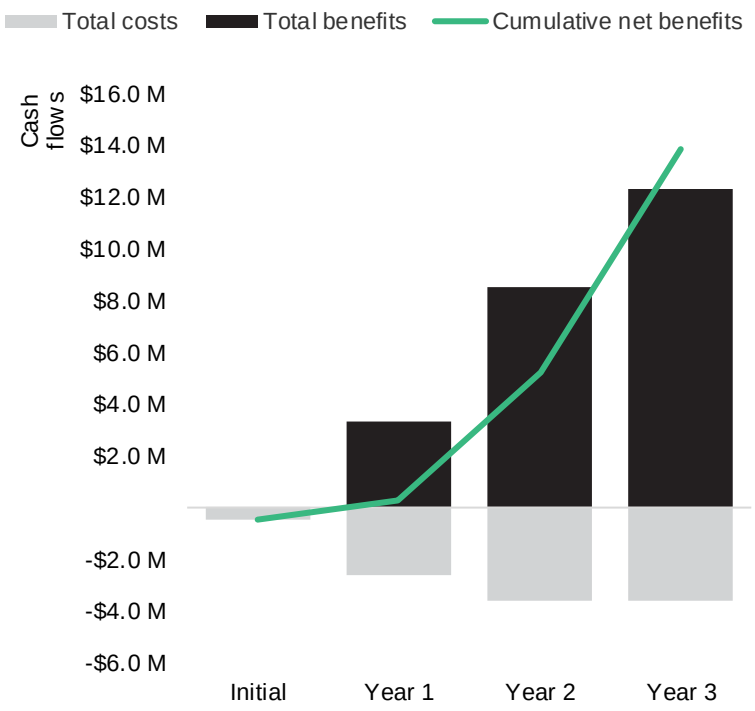
Protegrity Licensing Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Protegrity licensing	Forrester assumption	$0	$1,250,000	$2,500,000	$2,500,000
G2	Protegrity professional services	Forrester assumption	$0	$400,000	$50,000	
Gt	Protegrity licensing costs	G2	$0	$1,650,000	$2,550,000	$2,500,000
	Risk adjustment	↑5%				
Gtr	Protegrity licensing costs (risk-adjusted)		$0	$1,732,500	$2,677,500	$2,625,000
	Three-year total: $7,035,000			**Three-year present value: $5,760,011**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
	($465,534)	($2,607,054)	($3,627,270)	($3,640,332)	($10,340,190)	($8,568,362)
Total benefits	$0	$3,345,639	$8,565,227	$12,292,831	$24,203,697	$19,355,976
Net benefits	($465,534)	$738,585	$4,937,957	$8,652,499	$13,863,507	$10,787,614
ROI						126%
Payback						8 months

Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TOTAL ECONOMIC IMPACT APPROACH

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

PRESENT VALUE (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

NET PRESENT VALUE (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendix B: Supplemental Material

Related Forrester Research

"Now Tech: Data Security Platforms, Q1 2021," Forrester Research, Inc., February 25, 2021.

"Lay Your Security Tech Foundation," Forrester Research, Inc., January 11, 2021.

"The Forrester Wave™: Unstructured Data Security Platforms, Q2 2021," Forrester Research, Inc., May 17, 2021.

"Improve Cybersecurity And Privacy Oversight," Forrester Research Inc., December 17, 2021.

"Establish Your Security Technology Stack Foundation," Forrester Research, Inc., January 12, 2022.

Online Resources

For information related to global data privacy laws and regulations, the International Association of Privacy Professionals (IAPP) has resources available at https://iapp.org/.

Lothar Determann, "How data residency laws can harm privacy, commerce and innovation - and do little for national security," World Economic Forum, June 9, 2020 (https://www.weforum.org/agenda/2020/06/where-data-is-stored-could-impact-privacy-commerce-and-even-national-security-here-s-why/).

Nallan Sriraman, "Data Residency Laws Are Debilitating For Data Lakes, But That Doesn't Have To Be The Case," Forbes Technology Council, November 25, 2020 (https://www.forbes.com/sites/forbestechcouncil/2020/11/25/data-residency-laws-are-debilitating-for-data-lakes-but-that-doesnt-have-to-be-the-case/?sh=241ee3a738bb).

Appendix C: Endnotes

[1] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

[2] "Global Comprehensive Privacy Law Mapping Chart," International Association of Privacy Professionals, November 2021 (https://iapp.org/resources/article/global-comprehensive-privacy-law-mapping-chart/).


FORRESTER®